

Secrecy by Witness-Functions under Equational Theories

Jaouhar Fattahi

Department of Computer Sciences and
Software Engineering (LSI)
Laval University, Quebec, QC, Canada
jaouhar.fattahi.1@ulaval.ca

Mohamed Mejri

Department of Computer Sciences
and Software Engineering (LSI)
Laval University, Quebec, QC, Canada
mohamed.mejri@ift.ulaval.ca

Abstract—In this paper, we use the witness-functions to analyze cryptographic protocols for secrecy under nonempty equational theories. The witness-functions are safe metrics used to compute security. An analysis with a witness-function consists in making sure that the security of every atomic message does not decrease during its lifecycle in the protocol. The analysis gets more difficult under nonempty equational theories. Indeed, the intruder can take advantage of the algebraic properties of the cryptographic primitives to derive secrets. These properties arise from the use of mathematical functions, such as multiplication, addition, exclusive-or or modular exponentiation in the cryptosystems and the protocols. Here, we show how to use the witness-functions under nonempty equational theories and we run an analysis on the Needham-Schroeder-Lowe protocol under the cipher homomorphism. This analysis reveals that although this protocol is proved secure under the perfect encryption assumption, its security collapses under the homomorphic primitives. We show how the witness-functions help to illustrate an attack scenario on it and we propose an amended version to fix it.

Keywords- *Cryptographic protocols; Equational theories; Homomorphism; Secrecy.*

I. INTRODUCTION

In this paper, we use the witness-functions to statically analyze cryptographic protocols with respect to secrecy under nonempty equational theories. The Witness-Functions have been suggested by Fattahi et al. in [1]–[7] as metrics to attribute a safe value of security to each atomic message in the protocol. A protocol analysis with a witness-function consists in following every atomic message defined in the protocol and making sure that its value of security does not fall down during its lifecycle. In this case, the protocol is said to be increasing-so correct- with respect to secrecy. The use of cryptographic primitives with algebraic properties compels the verifier to undertake special precautions when using these functions since the cryptographic primitives supply the intruder with new redoubtable capabilities. We organize this paper as follows:

- First, we recall the theory of increasing protocols and we show that any protocol if proved increasing, using reliable metrics that meet few conditions, is correct with respect to secrecy;

- then, we present the witness-functions as reliable metrics and we show how to use them under nonempty equational theories;
- then, we run a formal analysis of the Needham-Schroeder-Lowe protocol and we show that although this protocol was proved correct under the perfect encryption assumption, it is no longer secure under the homomorphic primitives. We show that the witness-functions help to illustrate an attack scenario on it and we propose a corrected version of it based on hash functions;
- finally, we compare our method to some related works.

NOTATIONS

Here, we give the notations used throughout this paper.

- + We denote by $\mathcal{C} = \langle \mathcal{M}, \xi, \models, \mathcal{K}, \mathcal{L}^\exists, \ulcorner, \urcorner \rangle$ the context of verification containing the relevant parameters for a protocols analysis.
 - \mathcal{M} : is a set of messages built from the signature $\langle \mathcal{N}, \Sigma \rangle$ where \mathcal{N} is a set of atomic names (nonces, keys, principals, etc.) and Σ is a set of operators (\mathcal{E} : encryption, \mathcal{D} : decryption, $pair$: pairing (denoted by "." here), etc.). i.e. $\mathcal{M} = T_{\langle \mathcal{N}, \Sigma \rangle}(\mathcal{X})$. We use Γ to denote the set of substitution from \mathcal{X} to \mathcal{M} . We denote by \mathcal{A} the set of atomic messages in \mathcal{M} , by $\mathcal{A}(m)$ the set of atomic messages in m , by \mathcal{I} the set of agents (principals) in the protocol and by I the intruder. We denote by k^{-1} the reverse key of k and we assume that $(k^{-1})^{-1} = k$.
 - ξ : is the equational theory [8]–[11] that describes the algebraic properties of the operators in Σ by equations. For example, the homomorphic property is described by $\{m.m'\}_k = \{m\}_k.\{m'\}_k$ and the modular exponentiation property is described by $\{\{m\}_k\}_{k'} = \{\{m\}_{k'}\}_k$. Two messages m and m' that are equivalent under the equational theory ξ are denoted by $m =_\xi m'$.
 - \models : is the inference system of the intruder under the equational theory. Let M be a set of messages and m a single message. $M \models m$ expresses that the intruder is able to infer m from M using his capabilities. We extend that notation to valid traces as follows: $\rho \models$

m expresses the fact that the intruder can derive m from the trace ρ .

- \mathcal{K} : is a function from \mathcal{I} to \mathcal{M} , that attributes to any agent a set of atomic messages describing her initial knowledge. $K_C(I)$ denotes the initial knowledge of the intruder(or simply $K(I)$ where the context is evident).
 - \mathcal{L}^\sqsupset : is the security lattice $(\mathcal{L}, \sqsupset, \sqcup, \sqcap, \perp, \top)$ used to attribute a security level to a message. An example of a concrete lattice is $(2^{\mathcal{I}}, \subseteq, \cap, \cup, \mathcal{I}, \emptyset)$. We use this latter in this paper.
 - $\lceil \cdot \rceil$: is a partial function that attributes a value of security (type) to a message in \mathcal{M} . Let M be a set of messages and m be a sigle message. We express by $\lceil M \rceil \sqsupseteq \lceil m \rceil$ the fact $\exists m' \in M. \lceil m' \rceil \sqsupseteq \lceil m \rceil$
- + Let p be a protocol, we denote by $R_G(p)$ the set of the generalized roles of p . A generalized role is a protocol abstraction where the emphasis is put on a specific agent and where every unknown message by that agent and on which he cannot perform any verification is replaced by a variable. Further details on the role-based specification are available in [12]–[14]. We denote by \mathcal{M}_p^G the set of messages (ground terms and terms with variables) generated by $R_G(p)$, by \mathcal{M}_p the set of messages that are ground terms generated by substitution in the messages of \mathcal{M}_p^G . We denote by R^- (respectively R^+) the set of received messages (respectively sent messages) by an agent in the role R . By convention, we reserve the uppercases for sets or sequences and lowercases for single items. For instance, M denotes a set of messages, m a message, R a role consisting of a sequence of steps, r a single step and $R.r$ the role ending by the single step r .
- + A valid trace is a ground term obtained by substituting a non ground term in the generalized roles. We denote by $\llbracket p \rrbracket$ the infinite set of valid traces.
- + We assume that the intruder has the full-control of the net as described in the Dolev-Yao model [15]. We suppose no limitation neither on the length of messages nor on the number of interleaving sessions.

II. ABOUT THE CORRECTNESS OF INCREASING PROTOCOLS

Hereafter, we recall a major result of the increasing protocols [1], [4]: an increasing protocol is correct with respect to secrecy. For that, we need reliable metrics (functions) to estimate the security of the atomic messages of a protocol. To be reliable, a metric should meet few conditions. Here, we give these conditions and we substantiate the correctness of increasing protocols.

A. Reliable Functions

Definition II.1. (Well-formed Function) Let F be a function and \mathcal{C} be a context of verification. F is \mathcal{C} -

well-formed iff: $\forall M, M_1, M_2 \subseteq \mathcal{M}, \forall \alpha \in \mathcal{A}(\mathcal{M})$:

$$\begin{cases} F(\alpha, \{\alpha\}) = \perp; \\ F(\alpha, M_1 \cup M_2) = F(\alpha, M_1) \sqcap F(\alpha, M_2); \\ F(\alpha, M) = \top, \text{ if } \alpha \notin \mathcal{A}(M). \end{cases}$$

A well-formed function F should return the bottom value in the lattice for an atom α that appears in clear in M to express the fact that is exposed to everybody in M . It should return for it in the union of two sets, the minimum of the two values calculated in each set alone. It returns the top value in the lattice for any atom α that does appear in M to express the fact that none could derive it from M .

Definition II.2. (Full-Invariant-by-Intruder Function) Let F be a function and \mathcal{C} be a context of verification. F is \mathcal{C} -full-invariant-by-intruder iff:

$$\forall M \subseteq \mathcal{M}, m \in \mathcal{M}. M \models_{\mathcal{C}} m \Rightarrow \forall \alpha \in \mathcal{A}(m). (F(\alpha, m) \sqsupseteq F(\alpha, M)) \vee (\lceil K(I) \rceil \sqsupseteq \lceil \alpha \rceil).$$

An full-invariant-by-intruder function F is such that, when it affects a security value to an atom α in a set of messages M the intruder can never deduce from M , using his capabilities, another message m in which this value decreases (i.e. $F(\alpha, m) \not\sqsupseteq F(\alpha, M)$), except when α is deliberately destined to the intruder (i.e. $\lceil K(I) \rceil \sqsupseteq \lceil \alpha \rceil$).

Definition II.3. (Reliable Function) Let F be a function and \mathcal{C} be a context of verification.

$$F \text{ is } \mathcal{C}\text{-reliable} \text{ iff } \begin{cases} F \text{ is } \mathcal{C}\text{-well-formed} \\ F \text{ is } \mathcal{C}\text{-full-invariant-by-intruder} \end{cases}$$

A reliable function F is well-formed and full-invariant-by-intruder.

Definition II.4. (F -Increasing Protocol) Let F be a function, \mathcal{C} be a context of verification and p be a protocol.

p is F -increasing in \mathcal{C} iff:

$$\forall R.r \in R_G(p), \forall \sigma \in \Gamma : \mathcal{X} \rightarrow \mathcal{M}_p \text{ we have:}$$

$$\forall \alpha \in \mathcal{A}(\mathcal{M}). F(\alpha, r^+ \sigma) \sqsupseteq \lceil \alpha \rceil \sqcap F(\alpha, R^- \sigma)$$

An F -increasing protocol generates permanently strings such that every atomic message in has always a security value, computed by F , higher in the sent message (i.e. in $r^+ \sigma$) than it was in the received messages (i.e. in $R^- \sigma$).

Theorem II.5. (Correctness of Increasing Protocols) Let F be a \mathcal{C} -reliable Function and p an F -increasing protocol.

p is correct with respect to secrecy.

Theorem II.5 states that a protocol is correct with respect to secrecy when it is increasing using a reliable metric F to compute security. Hence, if the intruder manages to obtain a secret α , then its value computed by F is the bottom value in the lattice because F is well-formed. This could not arise because of the protocol rules because the protocol is increasing on F unless the value of security of α is the bottom from the beginning. In this case, α is not a secret. That could not arise using the capabilities of the intruder neither since F is full-invariant-by-intruder. Hence, the secret cannot be revealed. For further details on the proof, please see [4].

III. BUILDING RELIABLE FUNCTIONS UNDER EQUATIONAL THEORIES

A. Reliable Selections Under the Perfect Encryption Assumption

In [1] we propose an abstract class of reliable selections under the perfect encryption assumption that we denote by S_{Gen}^{EK} . Each selection S in S_{Gen}^{EK} should return for an atom α in a message m :

- 1) if α is encrypted by a key k such that k is the most external key satisfying the condition $\lceil k^{-1} \rceil \supseteq \lceil \alpha \rceil$ (we call it the external protective key), a subset among k^{-1} and the atoms that travel with α under the same protection by k (α itself is not selected);
- 2) for two messages joined by a function f in Σ such that f is not an encryption by the external protective key (e.g. pair), the union of the two subselections performed in each message separately.
- 3) if α does not have a protective key in m , the bottom value in the lattice (all the atoms);
- 4) if α does not appear in m , the top value in the lattice (the empty set);

From the abstract class S_{Gen}^{EK} , we propose three useful selections:

- 1) the selection S_{MAX}^{EK} : returns for an atom α in a message m encrypted by the external protective key k , all the principal identities under the same protection by k , in addition to k^{-1} ;
- 2) the selection S_{EK}^{EK} : returns for an atom α in a message m encrypted by the external protective key k , only the key k^{-1} ;
- 3) the selection S_N^{EK} : returns for an atom α in a message m encrypted by the external protective key k , all the principal identities under the same protection by k ;

B. Reliable Selections Under Equational Theories

In nonempty equational theories [8]–[11], cryptographic primitives have algebraic properties that arise from the use of mathematical functions like multiplication, addition, exclusive-or or modular exponentiation in cryptosystems and protocols. In Example III.1 we provide some of these algebraic properties.

Example III.1. (Some Algebraic Properties)

- Homomorphism: is the property that leads to have an equivalence between the two terms $\{m.m'\}_k$ and $\{m\}_k.\{m'\}_k$. That is the case of the RSA public key cryptosystems, the ElGamal cryptosystem, the Brakerski-Gentry-Vaikuntanathan cryptosystem, the NTRU-based cryptosystem, the Gentry-Sahai-Waters cryptosystem, the Goldwasser-Micali cryptosystem, etc;
- Modular exponentiation: is the property that leads to have an equivalence between the two terms $\{\{m\}_k\}_{k'}$ and $\{\{m\}_{k'}\}_k$. This is the case of the Diffie-Hellman key agreement protocol;

- XOR cipher: in many encryption algorithms, a plaintext is encrypted by applying the bitwise XOR operator to each character using some key k . To decrypt the output, applying the XOR function over with the key will cancel out the cipher. The XOR operator is vulnerable to a known attack since plaintext XOR ciphertext = k ;
- Etc.

These properties endow the intruder with additional capabilities to manipulate the protocol.

Condition III.2. (Normal form with the smallest selection) Let S be a selection of the class S_{Gen}^{EK} and \mathcal{C} be a context of verification. Let's have a rewriting system \rightarrow_ξ such that $\forall m \in \mathcal{M}, \forall \alpha \in \mathcal{A}(m) \wedge \alpha \notin \text{Clear}(m)$, we have:

$$\forall l \rightarrow r \in \rightarrow_\xi, S(\alpha, r) \subseteq S(\alpha, l)$$

We denote by m_\downarrow the normal form of m in \rightarrow_ξ .

The condition on the rewriting system is introduced to make sure that the selection in the normal form is the smallest among all forms of a given message. This prevents the selection S to select atoms that might be inserted maliciously by the intruder by manipulating the equational theory. Hence, we are sure that all selected atoms by S are honest and do not come by an intruder manipulation of the message. We assume that the equational theory in the context of verification allows always the extraction of a convergent rewriting system that meets Condition III.2. This is the case with the most of equational theories used in the literature [9]–[11].

Example III.3. Let $m = \{\alpha.C\}_{k_{ab}}$ be a message. Let us have a context of verification that includes the homomorphic cryptography (i.e. $\{\alpha.C\}_{k_{ab}} = \{\alpha\}_{k_{ab}}.\{C\}_{k_{ab}}$). In the form $\{\alpha.C\}_{k_{ab}}$, the selection $S(\alpha, \{\alpha.C\}_{k_{ab}})$ can select C , but in the form $\{\alpha\}_{k_{ab}}.\{C\}_{k_{ab}}$, the selection $S(\alpha, \{\alpha\}_{k_{ab}}.\{C\}_{k_{ab}})$ cannot. We orient so the rewriting system so that it returns the form $\{\alpha\}_{k_{ab}}.\{C\}_{k_{ab}}$ that is the normal form we choose.

C. From Selections to Reliable Functions Under Equational Theories

Having defined the selections above, we transform them now to security values. For that, we compose any selection S in S_{Gen}^{EK} with a suitable morphism ψ and this composition leads to a reliable function $F = \psi \circ S$. We define the morphism as follows:

- 1) it returns for a principal, its identity;
- 2) it returns for a key k^{-1} , if selected, the set of principals that know it in the context of verification.

We denote by F_{MAX}^{EK} , F_{EK}^{EK} and F_N^{EK} respectively the functions resulting from the compositions $\psi \circ S_{MAX}^{EK}$, $\psi \circ S_{EK}^{EK}$ and $\psi \circ S_N^{EK}$ and we prove that these functions are \mathcal{C} -reliable. The main idea of the proof is that the selection for any secret α in a message is carried out in an invariant zone (piece of message) that could not be augmented by the intruder using the equational theory seeing that the rewriting system is oriented in such way that the used form of a message is the smallest and

contains always honest atoms only. This zone is in addition protected by a protective key k that meets the condition $\lceil K(I) \rceil \sqsupseteq \lceil k^{-1} \rceil$. That means, to alter this zone (to decrease the security level of α), the intruder should have derived the atomic key k^{-1} in advance. So, in this stage of the proof, his knowledge should satisfy the condition $\lceil K(I) \rceil \sqsupseteq \lceil k^{-1} \rceil$. Since the key k^{-1} satisfies the condition $\lceil k^{-1} \rceil \sqsupseteq \lceil \alpha \rceil$ then the knowledge of the intruder should satisfy the condition $\lceil K(I) \rceil \sqsupseteq \lceil \alpha \rceil$ too by transitivity of the order " \sqsupseteq " in a lattice. This is accurately the definition of a full-invariant-by-intruder function. Furthermore, these functions are also well-formed by construction. Then, they are reliable.

Example III.4. Let α be an atom, m be a message and k_{ab} be a key such that: $\lceil \alpha \rceil = \{A, B, S\}$; $m = \{A.C.\{\alpha.D\}_{k_{as}}\}_{k_{ab}}$; $k_{ab}^{-1} = k_{ab}$, $k_{as}^{-1} = k_{as}$; $\lceil k_{as} \rceil = \{A, S\}$, $\lceil k_{ab} \rceil = \{A, B\}$;

Under the perfect encryption assumption (empty equational theory), we have:

$$\begin{aligned} S_{MAX}^{EK}(\alpha, m) &= S_{MAX}^{EK}(\alpha, \{A.C.\{\alpha.D\}_{k_{as}}\}_{k_{ab}}) = \\ &= \{A, C, D, k_{ab}^{-1}\}; \\ F_{MAX}^{EK}(\alpha, m) &= \psi \circ S_{MAX}^{EK}(\alpha, m) = \{A, C, D\} \sqcap \lceil k_{ab}^{-1} \rceil = \\ &= \{A, C, D\} \cup \{A, B\} = \{A, C, D, B\}. \end{aligned}$$

Under the cipher homomorphism, we have:

$$\begin{aligned} S_{MAX}^{EK}(\alpha, m) &= S_{MAX}^{EK}(\alpha, \{A.C.\{\alpha.D\}_{k_{as}}\}_{k_{ab}}) = \\ S_{MAX}^{EK}(\alpha, \{A\}_{k_{ab}} \cdot \{C\}_{k_{ab}} \cdot \{\{\alpha.D\}_{k_{as}}\}_{k_{ab}}) &= \\ S_{MAX}^{EK}(\alpha, \{A\}_{k_{ab}}) \cup S_{MAX}^{EK}(\alpha, \{C\}_{k_{ab}}) \cup &= \\ S_{MAX}^{EK}(\alpha, \{\{\alpha\}_{k_{as}}\}_{k_{ab}}) \cup S_{MAX}^{EK}(\alpha, \{\{D\}_{k_{as}}\}_{k_{ab}}) &= \\ \emptyset \cup \emptyset \cup \{k_{ab}^{-1}\} \cup \emptyset = \{k_{ab}^{-1}\}; & \end{aligned}$$

$$F_{MAX}^{EK}(\alpha, m) = \psi \circ S_{MAX}^{EK}(\alpha, m) = \lceil k_{ab}^{-1} \rceil = \{A, B\}.$$

In the rest of this paper, we denote by F any of the functions F_{MAX}^{EK} , F_{EK}^{EK} and F_N^{EK} .

IV. THE WITNESS-FUNCTIONS

From Theorem II.5, if a protocol p is confirmed F -increasing on its *valid traces* using a reliable function F , then it is correct with respect to secrecy. However, the set of traces is not finite. In order to be able to analyze a protocol on its finite set of the generalized roles, we have to readjust the reliable function so that it can deal with the problem of substitution and we seek an extra mechanism that enables us to pass from the decision made on the generalized roles to the same decision on the ground terms of the valid traces. The witness-functions are designed for that purpose. But first, let us instill the notion of derivative messages. A derivative message is a term in the generalized roles from which we rule out the variables. This is described by Definition IV.1.

Definition IV.1. (Derivation) A derivative message is defined as follows:

$$\begin{aligned} \partial_X \alpha &= \alpha \\ \partial_X \epsilon &= \epsilon \\ \partial_X X &= \epsilon \\ \partial_X Y &= Y \\ \partial_{\{X\}} m &= \partial_X m \\ \partial_{[X]} m &= \partial_{\{x_m \setminus X\}} m \\ \partial_X f(m) &= f(\partial_X m), f \in \Sigma \\ \partial_{S_1 \cup S_2} m &= \partial_{S_1} \partial_{S_2} m \end{aligned}$$

The idea now is to apply a reliable function F to derivative messages instead of the message itself. For an atom in the static part of a message (i.e. in ∂m), we compute its security with no respect to variables. Else, for any content coming by substitution of a variable X , it is computed as the variable itself treated as a constant block. This is motivated by the fact that if the security of the block substituting X does not decrease, then the whole block (the global secret $X\sigma$) is never revealed and hence any sub-secret in it is never revealed. This is given by Definition IV.2.

Definition IV.2. Let $m \in \mathcal{M}_p^G$, $X \in \mathcal{X}_m$ and $m\sigma$ be a valid trace. For all $\alpha \in \mathcal{A}(m\sigma)$, $\sigma \in \Gamma$, we denote by:

$$F(\alpha, \partial[\bar{\alpha}]m\sigma) = \begin{cases} F(\alpha, \partial m) & \text{if } \alpha \in \mathcal{A}(\partial m), \\ F(X, \partial[X]m) & \text{if } \alpha \notin \mathcal{A}(\partial m) \\ & \text{and } \alpha \in \mathcal{A}(X\sigma). \end{cases}$$

The application in Definition IV.2 could not still be used to analyze protocols since derivation has a serious undesirable side-effect. Let have a look at Example IV.3:

Example IV.3. Let m_1 and m_2 be two messages of \mathcal{M}_p^G such that $m_1 = \{X.\alpha.D\}_{k_{ab}}$ and $m_2 = \{C.\alpha.Y\}_{k_{ab}}$ and $\lceil \alpha \rceil = \{A, B\}$. Let $m = \{C.\alpha.D\}_{k_{ab}}$ be in a valid trace.

$$F_{MAX}^{EK}(\alpha, \partial[\bar{\alpha}]m) = \begin{cases} \{A, B, D\}, & \text{if } m = m_1\sigma_1 | X\sigma_1 = C, \\ \{A, B, C\}, & \text{if } m = m_2\sigma_2 | Y\sigma_2 = D \end{cases}$$

Thus, $F_{MAX}^{EK}(\alpha, \partial[\bar{\alpha}]m)$ is not even a function. (i.e. it may return more than one value to the same input).

The witness-function in Definition IV.4 fixes this bug: it looks for all the sources of $m\sigma$, applies the application in Definition IV.2 and returns the minimum. This minimum must exist and is unique in a lattice.

Definition IV.4. (Witness-Function) Let $m \in \mathcal{M}_p^G$, $X \in \mathcal{X}_m$ and $m\sigma$ be a valid trace. Let p be a protocol and F be a \mathcal{C} -reliable Function. We define a witness-function $\mathcal{W}_{p,F}$ for all $\alpha \in \mathcal{A}(m\sigma)$, $\sigma \in \Gamma$, as follows:

$$\mathcal{W}_{p,F}(\alpha, m\sigma) = \sqcap_{\substack{m' \in \mathcal{M}_p^G \\ \exists \sigma' \in \Gamma. m'\sigma' = m\sigma}} F(\alpha, \partial[\bar{\alpha}]m'\sigma')$$

A witness-function $\mathcal{W}_{p,F}$ is reliable when F is reliable. In fact, it is easy to see that it is well-formed. It is also full-invariant-by-intruder as the returned values (principal identities) are those returned by F on derivative messages of the sources of $m\sigma$ and derivation does not add new candidates, it just takes away some of them (that come by substitution), but

the message $A.B.\{X\}_{k_b}$. This is described by the following rules:

$$S^i : \frac{\Box}{\{N_a^\alpha.A\}_{k_b}} \quad S^j : \frac{\{B.N_a^\alpha\}_{k_a}.\{B.X\}_{k_a}}{A.B.\{X\}_{k_b}}$$

Analysis of the messages exchanged in the session S^i :

1- For N_a^α :

a- On sending: $r_{S^i}^+ = \{N_a^\alpha.A\}_{k_b}$ (in a sending step, the lower-bound is used)

$$\begin{aligned} & N_a^\alpha.\{m' \in \mathcal{M}_p^G | \exists \sigma' \in \Gamma.\sigma'm' = \sigma'r_{S^i}^+\} \\ &= N_a^\alpha.\{m' \in \mathcal{M}_p^G | \exists \sigma' \in \Gamma.m'\sigma' = \{N_a^\alpha.A\}_{k_b}\sigma'\} \\ &= \{(\{N_{A_1}.A_1\}_{k_{B_1}}, \sigma'_1), (\{X_2\}_{k_{B_4}}, \sigma'_2), (\{Y_1.A_4\}_{k_{B_5}}, \sigma'_3)\} \end{aligned}$$

such that:

$$\begin{cases} \sigma'_1 = \{N_{A_1} \mapsto N_a^\alpha, A_1 \mapsto A, k_{B_1} \mapsto k_b\} \\ \sigma'_2 = \{X_2 \mapsto N_a^\alpha.A, k_{B_4} \mapsto k_b\} \\ \sigma'_3 = \{Y_1 \mapsto N_a^\alpha.A_4 \mapsto A, k_{B_5} \mapsto k_b\} \end{cases}$$

$$\begin{aligned} & \mathcal{W}'_{p,F}(N_a^\alpha, \{N_a^\alpha.A\}_{k_b}) \\ &= \{\text{Definition of the lower-bound of the witness-function}\} \\ & F(N_a^\alpha, \partial[\overline{N_a^\alpha}]\{N_{A_1}.A_1\}_{k_{B_1}}\sigma'_1) \sqcap F(N_a^\alpha, \partial[\overline{N_a^\alpha}]\{X_2\}_{k_{B_4}}\sigma'_2) \sqcap \\ & F(N_a^\alpha, \partial[\overline{N_a^\alpha}]\{Y_1.A_4\}_{k_{B_5}}\sigma'_3) \\ &= \{\text{Setting the static neighborhood}\} \\ & F(N_a^\alpha, \partial[\overline{N_a^\alpha}]\{N_a^\alpha.A\}_{k_b}\sigma'_1) \sqcap F(N_a^\alpha, \partial[\overline{N_a^\alpha}]\{X_2\}_{k_b}\sigma'_2) \sqcap \\ & F(N_a^\alpha, \partial[\overline{N_a^\alpha}]\{Y_1.A\}_{k_b}\sigma'_3) \\ &= \{\text{Definition IV.2}\} \\ & F(N_a^\alpha, \{N_a^\alpha.A\}_{k_b}) \sqcap F(X_2, \partial[\overline{X_2}]\{X_2\}_{k_b}) \sqcap \\ & F(Y_1, \partial[\overline{Y_1}]\{Y_1.A\}_{k_b}) \\ &= \{\text{Definition IV.1}\} \\ & F(N_a^\alpha, \{N_a^\alpha.A\}_{k_b}) \sqcap F(X_2, \{X_2\}_{k_b}) \sqcap F(Y_1, \{Y_1.A\}_{k_b}) \\ &= \{\text{Normal form under homomorphism}\} \\ & F(N_a^\alpha, \{N_a^\alpha\}_{k_b}) \sqcap F(N_a^\alpha, \{A\}_{k_b}) \sqcap F(X_2, \{X_2\}_{k_b}) \sqcap \\ & F(Y_1, \{Y_1\}_{k_b}) \sqcap F(Y_1, \{A\}_{k_b}) \\ &= \{\text{Since } F = F_{MAX}^{EK}\} \\ & \{B\} \sqcap \top \sqcap \{B\} \sqcap \{B\} \sqcap \top = \{B\} \quad (1.0) \end{aligned}$$

b- On receiving: $R_{S^i}^- = \emptyset$ (in a receiving step, the upper-bound is used)

$$F(N_a^\alpha, \partial[\overline{N_a^\alpha}]\emptyset) = F(N_a^\alpha, \emptyset) = \top \quad (1.1)$$

2- Conformity with Theorem IV.6:

$$\begin{aligned} & \text{From (1.0) and (1.1), we have: } \mathcal{W}'_{p,F}(N_a^\alpha, \{N_a^\alpha.A\}_{k_b}) = \\ & \{B\} \sqsupseteq \lceil N_a^\alpha \rceil \sqcap F(N_a^\alpha, \partial[\overline{N_a^\alpha}]\emptyset) = \lceil N_a^\alpha \rceil \sqcap \top = \{A, B\} \quad (1.2) \end{aligned}$$

From (1.2) we have: the messages exchanged in the session S^i respect the correctness criterion set in Theorem IV.6. (I)

Analysis of the messages exchanged in the session S^j :

1- $\forall X$:

$$\begin{aligned} & \text{a- On sending: } r_{S^j}^+ = A.B.\{X\}_{k_b} \\ & \mathcal{W}'_{p,F}(X, A.B.\{X\}_{k_b}) = \mathcal{W}'_{p,F}(X, A) \sqcap \mathcal{W}'_{p,F}(X, B) \sqcap \\ & \mathcal{W}'_{p,F}(X, \{X\}_{k_b}) = \top \sqcap \top \sqcap \mathcal{W}'_{p,F}(X, \{X\}_{k_b}) = \\ & \mathcal{W}'_{p,F}(X, \{X\}_{k_b}) \quad (2.0) \end{aligned}$$

$$\begin{aligned} & \forall X.\{m' \in \mathcal{M}_p^G | \exists \sigma' \in \Gamma.m'\sigma' = \{X\}_{k_b}\sigma'\} \\ &= \{(\{X_2\}_{k_{B_4}}, \sigma'_1)\} \text{ such that:} \end{aligned}$$

$$\sigma'_1 = \{X_2 \mapsto X, k_{B_4} \mapsto k_b\}$$

$$\begin{aligned} & \mathcal{W}'_{p,F}(X, \{X\}_{k_b}) \\ &= \{\text{Definition of the lower-bound of the witness-function}\} \\ & F(X, \partial[\overline{X}]\{X_2\}_{k_{B_4}}\sigma'_1) \\ &= \{\text{Setting the static neighborhood}\} \\ & F(X, \partial[\overline{X}]\{X_2\}_{k_b}\sigma'_1) \\ &= \{\text{Definition IV.2}\} \\ & F(X_2, \partial[\overline{X_2}]\{X_2\}_{k_b}) \\ &= \{\text{Definition IV.1}\} \\ & F(X_2, \{X_2\}_{k_b}) \\ &= \{\text{Normal form under homomorphism}\} \\ & F(X_2, \{X_2\}_{k_b}) \\ &= \{\text{Since } F = F_{MAX}^{EK}\} \\ & \{B\} \quad (2.1) \end{aligned}$$

b- On receiving: $R_{S^j}^- = \{B.N_a^\alpha\}_{k_a}.\{B.X\}_{k_a}$ (in a receiving step, the upper-bound is used)

$$\begin{aligned} & F(X, \partial[\overline{X}]\{B.N_a^\alpha\}_{k_a}.\{B.X\}_{k_a}) = F(X, \partial[\overline{X}]\{B.N_a^\alpha\}_{k_a}) \sqcap \\ & F(X, \partial[\overline{X}]\{B.X\}_{k_a}) = \\ & F(X, \{B.N_a^\alpha\}_{k_a}) \sqcap F(X, \{B.X\}_{k_a}) \\ &= \{\text{Normal form under homomorphism}\} \\ & F(X, \{B\}_{k_a}) \sqcap F(X, \{N_a^\alpha\}_{k_a}) \sqcap F(X, \{B\}_{k_a}) \sqcap \\ & F(X, \{X\}_{k_a}) = \\ & \top \sqcap \top \sqcap \top \sqcap \{A\} = \{A\} \quad (2.2) \end{aligned}$$

3-Conformity with Theorem IV.6:

From (2.0), (2.1) and (2.2), we have:

$$\begin{aligned} & \mathcal{W}'_{p,F}(X, A.B.\{X\}_{k_b}) = \{B\} \not\sqsupseteq \lceil X \rceil \sqcap \\ & F(X, \partial[\overline{X}]\{B.N_a^\alpha\}_{k_a}.\{B.X\}_{k_a}) = \lceil X \rceil \sqcup \{A\} \quad (2.3) \end{aligned}$$

From (2.3), we have: the messages exchanged in the session S^j do not respect the correctness criterion set in Theorem IV.6. (II)

From (I) and (II), the messages exchanged in the generalized role of A do not respect the correctness criterion set in Theorem IV.6. (III)

B. Analysis of the generalized role of B

As defined in the generalized roles of p , an agent B can participate in a session S'^i , in which he receives the message $\{Y.A\}_{k_b}$ and he sends the message $\{B.Y\}_{k_a}.\{B.N_b^\alpha\}_{k_a}$. This is described by the following rule:

$$S'^i : \frac{\{Y.A\}_{k_b}}{\{B.Y\}_{k_a}.\{B.N_b^\alpha\}_{k_a}}$$

1- For N_b^α :

a- On sending: $r_{S'^i}^+ = \{B.Y\}_{k_a}.\{B.N_b^\alpha\}_{k_a}$ (in a sending step, the lower-bound is used)

$$\begin{aligned} & \mathcal{W}'_{p,F}(N_b^\alpha, \{B.Y\}_{k_a}.\{B.N_b^\alpha\}_{k_a}) = \mathcal{W}'_{p,F}(N_b^\alpha, \{B.Y\}_{k_a}) \sqcap \\ & \mathcal{W}'_{p,F}(N_b^\alpha, \{B.N_b^\alpha\}_{k_a}) = \\ & \top \sqcap \mathcal{W}'_{p,F}(N_b^\alpha, \{B.N_b^\alpha\}_{k_a}) = \mathcal{W}'_{p,F}(N_b^\alpha, \{B.N_b^\alpha\}_{k_a}) \quad (3.0) \\ & \forall N_b^\alpha.\{m' \in \mathcal{M}_p^G | \exists \sigma' \in \Gamma.m'\sigma' = \{B.N_b^\alpha\}_{k_a}\sigma'\} \end{aligned}$$

$= \{(\{B_3.X_1\}_{k_{A_3}}, \sigma'_1), (\{X_2\}_{k_{B_4}}, \sigma'_2), (\{B_7.N_{B_7}\}_{k_{A_6}}, \sigma'_3)\}$
such that:

$$\begin{cases} \sigma'_1 = \{B_3 \mapsto B, X_1 \mapsto N_b^\alpha, k_{A_3} \mapsto k_a\} \\ \sigma'_2 = \{X_2 \mapsto B.N_b^\alpha, k_{B_4} \mapsto k_a\} \\ \sigma'_3 = \{B_7 \mapsto B, N_{B_7} \mapsto N_b^\alpha, k_{A_6} \mapsto k_a\} \end{cases}$$

$$\begin{aligned} & \mathcal{W}'_{p,F}(N_b^\alpha, \{B.N_b^\alpha\}_{k_a}) \\ &= \{\text{Definition of the lower-bound of the witness-function}\} \\ & F(N_b^\alpha, \partial[\overline{N_b^\alpha}]\{B_3.X_1\}_{k_{A_3}} \sigma'_1) \quad \sqcap \\ & F(N_b^\alpha, \partial[\overline{N_b^\alpha}]\{X_2\}_{k_{B_4}} \sigma'_2) \sqcap F(N_b^\alpha, \partial[\overline{N_b^\alpha}]\{B_7.N_{B_7}\}_{k_{A_6}} \sigma'_3) \\ &= \{\text{Setting the static neighborhood}\} \\ & F(N_b^\alpha, \partial[\overline{N_b^\alpha}]\{B.X_1\}_{k_a} \sigma'_1) \quad \sqcap \\ & F(N_b^\alpha, \partial[\overline{N_b^\alpha}]\{X_2\}_{k_a} \sigma'_2) \sqcap F(N_b^\alpha, \partial[\overline{N_b^\alpha}]\{B.N_b^\alpha\}_{k_a} \sigma'_3) \\ &= \{\text{Definition IV.2}\} \\ & F(X_1, \partial[\overline{X_1}]\{B.X_1\}_{k_a}) \quad \sqcap \quad F(X_2, \partial[\overline{X_2}]\{X_2\}_{k_a}) \quad \sqcap \\ & F(N_b^\alpha, \partial[\overline{N_b^\alpha}]\{B.N_b^\alpha\}_{k_a}) \\ &= \{\text{Definition IV.1}\} \\ & F(X_1, \{B.X_1\}_{k_a}) \sqcap F(X_2, \{X_2\}_{k_a}) \sqcap F(N_b^\alpha, \{B.N_b^\alpha\}_{k_a}) \\ &= \{\text{Normal form under homomorphism}\} \\ & F(X_1, \{B\}_{k_a}) \sqcap F(X_1, \{X_1\}_{k_a}) \sqcap F(X_2, \{X_2\}_{k_a}) \sqcap \\ & F(N_b^\alpha, \{B\}_{k_a}) \sqcap F(N_b^\alpha, \{N_b^\alpha\}_{k_a}) \\ &= \{\text{Since } F = F_{MAX}^{EK}\} \\ & \top \sqcap \{A\} \sqcap \{A\} \sqcap \{A\} \sqcap \top \sqcap \{A\} = \{A\} \quad (3.1) \end{aligned}$$

b- On receiving: $R_{S',i}^- = \{Y.A\}_{k_b}$ (in a receiving step, the upper-bound is used)

$$F(N_b^\alpha, \partial[\overline{N_b^\alpha}]\{Y.A\}_{k_b}) = F(N_b^\alpha, \{A\}_{k_b}) = \top \quad (3.2)$$

2- $\forall Y$:

a- On sending: $r_{S',i}^+ = \{B.Y\}_{k_a} \cdot \{B.N_b^\alpha\}_{k_a}$ (in a receiving step, the upper-bound is used)

$$\begin{aligned} & \mathcal{W}'_{p,F}(Y, \{B.Y\}_{k_a} \cdot \{B.N_b^\alpha\}_{k_a}) = \mathcal{W}'_{p,F}(Y, \{B.Y\}_{k_a}) \sqcap \\ & \mathcal{W}'_{p,F}(Y, \{B.N_b^\alpha\}_{k_a}) = \\ & \mathcal{W}'_{p,F}(Y, \{B.Y\}_{k_a}) \sqcap \top = \mathcal{W}'_{p,F}(Y, \{B.Y\}_{k_a}) \quad (3.3) \end{aligned}$$

$$\begin{aligned} & \forall Y. \{m' \in \mathcal{M}_p^G \mid \exists \sigma' \in \Gamma. m' \sigma' = \{B.Y\}_{k_a} \sigma'\} \\ &= \{(\{B_3.X_1\}_{k_{A_3}}, \sigma_1), (\{X_2\}_{k_{B_4}}, \sigma_2)\} \text{ such that:} \end{aligned}$$

$$\begin{cases} \sigma'_1 = \{B_3 \mapsto B, X_1 \mapsto Y, k_{A_3} \mapsto k_a\} \\ \sigma'_2 = \{X_2 \mapsto B.Y, k_{B_4} \mapsto k_a\} \end{cases}$$

$$\begin{aligned} & \mathcal{W}'_{p,F}(Y, \{B.Y\}_{k_a}) \\ &= \{\text{Definition of the lower-bound of the witness-function}\} \\ & F(Y, \partial[\overline{Y}]\{B_3.X_1\}_{k_{A_3}} \sigma'_1) \sqcap F(Y, \partial[\overline{Y}]\{X_2\}_{k_{B_4}} \sigma'_2) \\ &= \{\text{Setting the static neighborhood}\} \\ & F(Y, \partial[\overline{Y}]\{B.X_1\}_{k_a} \sigma'_1) \sqcap F(Y, \partial[\overline{Y}]\{X_2\}_{k_a} \sigma'_2) = \\ &= \{\text{Definition IV.2}\} \\ & F(X_1, \partial[\overline{X_1}]\{B.X_1\}_{k_a}) \sqcap F(X_2, \partial[\overline{X_2}]\{X_2\}_{k_a}) \\ &= \{\text{Definition IV.1}\} \\ & F(X_1, \{B.X_1\}_{k_a}) \sqcap F(X_2, \{X_2\}_{k_a}) \\ &= \{\text{Normal form under homomorphism}\} \\ & F(X_1, \{B\}_{k_a}) \sqcap F(X_1, \{X_1\}_{k_a}) \sqcap F(X_2, \{X_2\}_{k_a}) \\ &= \{\text{Since } F = F_{MAX}^{EK}\} \\ & \top \sqcap \{A\} \sqcap \{A\} = \{A\} \quad (3.4) \end{aligned}$$

b- On receiving: $R_{S',i}^- = \{Y.A\}_{k_b}$ (in a receiving step, the upper-bound is used)

$$\begin{aligned} & F(Y, \partial[\overline{Y}]\{Y.A\}_{k_b}) = F(Y, \{Y.A\}_{k_b}) = \\ & \{\text{Normal form under homomorphism}\} \\ & F(Y, \{Y\}_{k_b}) \sqcap F(Y, \{A\}_{k_b}) = \{B\} \sqcap \top = \{B\} \quad (3.5) \end{aligned}$$

3- Conformity with Theorem IV.6:

From (3.0), (3.1) and (3.2) we have:

$$\mathcal{W}'_{p,F}(N_b^\alpha, \{B.Y\}_{k_a} \cdot \{B.N_b^\alpha\}_{k_a}) = \{A\} \sqsupseteq \lceil N_b^\alpha \rceil \sqcap F(N_b^\alpha, \partial[\overline{N_b^\alpha}]\{Y.A\}_{k_b}) = \{A, B\} \quad (3.6)$$

From (3.3), (3.4) and (3.5) we have:

$$\mathcal{W}'_{p,F}(Y, \{B.Y\}_{k_a} \cdot \{B.N_b^\alpha\}_{k_a}) = \{A\} \not\sqsupseteq \lceil Y \rceil \sqcap F(Y, \partial[\overline{Y}]\{Y.A\}_{k_b}) = \lceil Y \rceil \sqcap \{B\} \quad (3.7)$$

From (3.7), the messages exchanged in the session S'^i do not respect the correctness criterion set in Theorem IV.6. (IV)

From (IV), the messages exchanged in the generalized role of B do not respect the correctness criterion stated Theorem IV.6. (V)

C. Results and interpretation

The results of the analysis of the Needham-Schroeder-Lowe protocol under homomorphism are summarized in Table II.

	α	Role	R^-	r^+	Theo.IV.6
1	N_a^α	A	\emptyset	$\{N_a^\alpha.A\}_{k_b}$	✓
2	$\forall X$	A	$\{B.N_a^\alpha\}_{k_a} \cdot \{B.X\}_{k_a}$	$A.B \cdot \{X\}_{k_b}$	✗
3	$\forall Y$	B	$\{A.Y\}_{k_b}$	$\{B.Y\}_{k_a} \cdot \{B.N_b^\alpha\}_{k_a}$	✗
4	N_b^α	B	$\{A.Y\}_{k_b}$	$\{B.Y\}_{k_a} \cdot \{B.N_b^\alpha\}_{k_a}$	✓

Table II: Conformity of the Needham-Schroeder-Lowe protocol with Theorem IV.6 under cipher homomorphism

From the rows (2) and (3) of Table II, the Needham-Schroeder-Lowe protocol under the homomorphic property is rejected by Theorem IV.6. Therefore, we conclude that it may involve a flaw with respect to secrecy. This flaw is described by Figure 1. In fact, an intruder can intercept the message $\{N_a^\alpha.A\}_{k_b}$ sent by a regular agent B to a regular agent A . Then, he concatenates it to the message $\{I\}_{k_b}$ that he creates by himself. The intruder knows in advance that the resulting message $\{N_a^\alpha.A\}_{k_b} \cdot \{I\}_{k_b}$ is equivalent to $\{N_a^\alpha.A.I\}_{k_b}$ under the homomorphic property. Then, he initiates a new session with B and sends him this resulting message. On reception, B understands the string $N_a^\alpha.A$ in the received message as a regular nonce N_I^β from a regular agent I starting a new session of the protocol since in a role-based specification this string corresponds to a variable Y on which he cannot perform any verification. B replies so by $\{B.N_a^\alpha.A\}_{k_i} \cdot \{B.N_b^\beta\}_{k_i}$. The intruder has just to decrypt it to get the secret N_a^α shared between A and B . The bounds of the used witness-function react well to this scenario and declares the drop of Y in the generalized role of B . That is because they base their calculation on the static neighborhood only. This neighborhood cannot be augmented by the intruder neither using his capabilities nor using the equational theory. The use of the normal form that gets rid of all the doubtful atoms is crucial for an analysis using the witness-functions under nonempty theories.

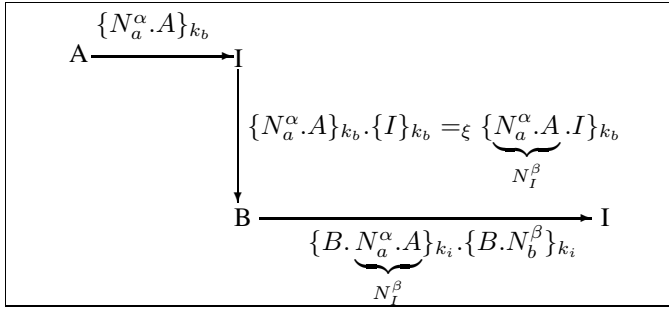


Figure 1: Attack on the Needham-Schroeder-Lowe protocol under cipher homomorphism

D. Proposal of an amended version

To correct this variant of the Needham-Schroeder-Lowe protocol, we propose the amended version in Table III. In this version, the nonces N_a and N_b are sent back concatenated with the sender and hashed by a secure hash function, $hash$. The receiver has just to compare the hashed values with $hash(sender.sent-nonce)$ to decide acceptance or rejection. Believing in the infeasibility to generate a message from its digest, the nonces are never derived and the protocol keeps its secrets.

$\langle 1, A \rightarrow B :$	$\{N_a . A\}_{k_b},$
$\langle 2, B \rightarrow A :$	$\{B . hash(B . N_a)\}_{k_a} . \{B . N_b\}_{k_a},$
$\langle 3, A \rightarrow B :$	$A . \{hash(A . N_b)\}_{k_b}.$

Table III: Amended version of the Needham-Schroeder-Lowe protocol (proposal)

VI. RELATED WORKS

Under nonempty equational theories, our witness-functions could be compared to the interpretation-functions of Houmani [16]–[19]. Unfortunately, these functions often fail to describe flaws inside protocols and simply report the protocol insecurity. They yield a high level of false negatives as well because they are not variable free in output. Contrariwise, the witness-functions are variable free in output owing to the derivation in its composition. We believe that our witness-functions are able to deal with other algebraic properties like the modular exponentiation property.

VII. CONCLUSION AND FUTURE WORK

In this paper, we presented how to use the witness-functions under nonempty equational theories to prove the correctness of cryptographic protocols with respect to secrecy. The major contribution is to adjust the witness-functions to deal with the algebraic properties in the equational theory through a judicious choice of the normal form on which we apply them. This normal form is obtained by a careful orientation of the rewriting system extracted from the theory. Afterwards, we successfully analyzed the Needham-Schroeder-Lowe protocol

under the homomorphic encryption and we clearly provided an attack scenario on it. In a future work, we intend to analyze more protocols under different theories [8]–[11].

NOTICE

© 2018 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works.

REFERENCES

- [1] Jaouhar Fattahi, Mohamed Mejri, and Hanane Houmani. Secrecy by witness functions. In *the 5th Proceedings of the Formal Methods for Security Workshop co-located with the PetriNets-2014 Conference*, volume 1158, pages 34–52. CEUR, 2014.
- [2] Jaouhar Fattahi, Mohamed Mejri, and Hanane Houmani. New functions for secrecy on real protocols. In *the Fourth International Conference on Computer Science, Engineering and Applications (ICCSEA 2014), Chennai, India*, pages 229–250. AIRCC, 2014.
- [3] J. Fattahi, M. Mejri, and H. Houmani. A Semi-Decidable Procedure for Secrecy in Cryptographic Protocols. *ArXiv e-prints*, August 2014.
- [4] Jaouhar Fattahi, Mohamed Mejri, and Hanane Houmani. Relaxed Conditions for Secrecy in a Role-Based specification. *International Journal of Information Security*, 1:33–36, July 2014.
- [5] Jaouhar Fattahi, Mohamed Mejri, and Hanane Houmani. Secrecy by witness-functions on increasing protocols. In *the 6th International Conference on Electronics, Computers and Artificial Intelligence (ECAI), Bucharest, Romania, October 2014*, pages 1–6. IEEE, 2014.
- [6] Jaouhar Fattahi, Mohamed Mejri, Moeiz Miraoui, and Hanane Houmani. Ensuring confidentiality in cryptographic protocols with the witness-functions. *International Journal of Computer and Communication Engineering*, 4(4):219–233, 2015.
- [7] Jaouhar Fattahi, Mohamed Mejri, and Hanane Houmani. Sufficient conditions for secrecy in cryptographic protocols. In *the World Symposium On Computer Networks and Information Security-WSCNIS'2014, Hammamet, Tunisia*, pages 14–32. NNGT, 2014.
- [8] Don Pigozzi. Universal equational theories and varieties of algebras. *Annals of Mathematical Logic*, 17(1–2):117 – 150, 1979.
- [9] Hubert Comon-Lundh, Véronique Cortier, and Eugen Zalinescu. Deciding security properties for cryptographic protocols. application to key cycles. *ACM Trans. Comput. Log.*, 11(2), 2010.
- [10] Véronique Cortier and Stéphanie Delaune. Decidability and combination results for two notions of knowledge in security protocols. *J. Autom. Reasoning*, 48(4):441–487, 2012.
- [11] Véronique Cortier, Steve Kremer, and Bogdan Warinschi. A survey of symbolic methods in computational analysis of cryptographic systems. *J. Autom. Reasoning*, 46(3–4):225–259, 2011.
- [12] Mourad Debbabi, Y. Legaré, and Mohamed Mejri. An environment for the specification and analysis of cryptoprotocols. In *ACSAC*, pages 321–332, 1998.
- [13] Mourad Debbabi, Mohamed Mejri, Nadia Tawbi, and I. Yahmadi. Formal automatic verification of authentication cryptographic protocols. In *ICFEM*, pages 50–59, 1997.
- [14] Mourad Debbabi, Mohamed Mejri, Nadia Tawbi, and I. Yahmadi. From protocol specifications to flaws and attack scenarios: An automatic and formal algorithm. In *WETICE*, pages 256–262, 1997.
- [15] Danny Dolev and Andrew Chi-Chih Yao. On the security of public key protocols. *IEEE Transactions on Information Theory*, 29(2):198–207, 1983.
- [16] Hanane Houmani and Mohamed Mejri. Practical and universal interpretation functions for secrecy. In *SECRYPT*, pages 157–164, 2007.
- [17] Hanane Houmani and Mohamed Mejri. Ensuring the correctness of cryptographic protocols with respect to secrecy. In *SECRYPT*, pages 184–189, 2008.
- [18] Hanane Houmani and Mohamed Mejri. Formal analysis of set and nsI protocols using the interpretation functions-based method. *Journal Comp. Netw. and Commun.*, 2012, 2012.

- [19] Hanane Houmani, Mohamed Mejri, and Hamido Fujita. Secrecy of cryptographic protocols under equational theory. *Knowl.-Based Syst.*, 22(3):160–173, 2009.
- [20] Stefan Ciobaca and Veronique Cortier. Protocol composition for arbitrary primitives. *2012 IEEE 25th Computer Security Foundations Symposium*, 0:322–336, 2010.
- [21] Véronique Cortier. Secure composition of protocols. In *TOSCA*, pages 29–32, 2011.
- [22] Véronique Cortier and Stéphanie Delaune. Safely composing security protocols. *Formal Methods in System Design*, 34(1):1–36, 2009.